Medical Care Collection Fund (MCCF) Electronic Data Interchange (EDI) Transaction Applications Suite (TAS) Phase 1

ePayments PRCA*4.5*317

Version 2

Deployment, Installation, Back-Out, and Rollback Guide

March 2017

Department of Veterans Affairs

Office of Information and Technology (OI&T)

Revision History

Date	Version	Description	Author
January 2017	1.0	Initial Version	Darlene White
March 2017	2.0	Changed cover page and footers to reflect that we are releasing this to the field in March 2017. Added test sites to section 3.2.2.	Darlene White

Artifact Rationale

This document describes the Deployment, Installation, Back-out, and Rollback Plan for new products going into the VA Enterprise. The plan includes information about system support, issue tracking, escalation processes, and roles and responsibilities involved in all those activities. Its purpose is to provide clients, stakeholders, and support personnel with a smooth transition to the new product or software, and should be structured appropriately, to reflect particulars of these procedures at a single or at multiple locations.

Per the Veteran-focused Integrated Process (VIP) Guide, the Deployment, Installation, Back-out, and Rollback Plan is required to be completed prior to Critical Decision Point #2 (CD #2), with the expectation that it will be updated throughout the lifecycle of the project for each build, as needed.

Table of Contents

1 Introduction

This document describes how to deploy and install the PRCA*4.5*317 as well as how to back-out the product and rollback to a previous version or data set.

1.1 Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom the PRCA*4.5*317 will be deployed and installed, as well as how it is to be backed out and rolled back, if necessary. The plan also identifies resources, communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document.

1.2 Dependencies

PRCA*4.5*304 must be installed **before** PRCA*4.5*317.

1.3 Constraints

This patch is intended for a fully patched VistA system.

2 Roles and Responsibilities

Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
1	VA OI&T, VA OI&T Health Product Support & PMO (Leidos)	Deployment	Plan and schedule deployment (including orchestration with vendors)	Planning
2	Local VAMC and CPAC processes	Deployment	Determine and document the roles and responsibilities of those involved in the deployment.	Planning
3	Field Testing (Initial Operating Capability - IOC), Health Product Support Testing & VIP Release Agent Approval	Deployment	Test for operational readiness	Testing
4	Health product Support and Field Operations	Deployment	Execute deployment	Deployment
5	Individual Veterans Administration Medical Centers (VAMCs)	Installation	Plan and schedule installation	Deployment

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
6	VIP Release Agent	Installation	Ensure authority to operate and that certificate authority security documentation is in place	Deployment
7	N/A for this patch as we are using only the existing VistA system	Installation	Validate through facility POC to ensure that IT equipment has been accepted using asset inventory processes	
8	VA's eBusiness team	Installations	Coordinate training	Deployment
9	VIP release Agent, Health Product Support & the development team	Back-out	Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out)	Deployment
10	No changes to current process – we are using the existing VistA system	Post Deployment	Hardware, Software and System Support	Warranty

3 Deployment

The deployment is planned as a national rollout.

This section provides the schedule and milestones for the deployment.

3.1 Timeline

The deployment and installation is scheduled to run for 30 days, as depicted in the master deployment schedule[1].

3.2 Site Readiness Assessment

This section discusses the locations that will receive the PRCA*4.5*317 deployment.

3.2.1 Deployment Topology (Targeted Architecture)

This patch PRCA*4.5*317 is to be nationally released to all VAMCs.

3.2.2 Site Information (Locations, Deployment Recipients)

The test sites for IOC testing are: Augusta, GA and Charleston, SC.

---

[1] Project schedule   (right click and select open hyperlink to access)
http://vaww.oed.portal.va.gov/pm/hape/ipt_5010/EDI_Portfolio/TAS%20Interim%20Repository/MCCF%20TAS%20Schedule.zip

- These sites will not be defined here until the sites have signed the Memorandum of Understanding (MOUs) and testing has completed as sometimes a site has to stop testing prior to the end of IOC.

Upon national release all VAMCs are expected to install this patch within the compliance date.

3.2.3 Site Preparation

The following table describes preparation required by the site prior to deployment.

Table 2: Site Preparation

Site/Other	Problem/Change Needed	Features to Adapt/Modify to New Product	Actions/Steps	Owner
N/A	N/A	N/A	N/A	N/A

3.3 Resources

3.3.1 Facility Specifics

The following table lists facility-specific features required for deployment.

Table 3: Facility-Specific Features

Site	Space/Room	Features Needed	Other
N/A	N/A	N/A	N/A

3.3.2 Hardware

The following table describes hardware specifications required at each site prior to deployment.

Table 4: Hardware Specifications

Required Hardware	Model	Version	Configuration	Manufacturer	Other
Existing VistA system	N/A	N/A	N/A	N/A	N/A

Please see the Roles and Responsibilities table in Section 2 for details about who is responsible for preparing the site to meet these hardware specifications.

3.3.3 Software

The following table describes software specifications required at each site prior to deployment.

Table 5: Software Specifications

Required Software	Make	Version	Configuration	Manufacturer	Other

Required Software	Make	Version	Configuration	Manufacturer	Other
Fully patched Accounts Receivable package within VistA	N/A	4.5	N/A	N/A	N/A
PRCA*4.5*304	N/A	Nationally released version	N/A	N/A	N/A

Please see the Roles and Responsibilities table in Section 2 above for details about who is responsible for preparing the site to meet these software specifications.

3.3.4 Communications

The sites that are participating in field testing (IOC) will use the "Patch Tracking" message in Outlook to communicate with the ePayments eBusiness team, the developers, and product support personnel.

3.3.4.1 Deployment/Installation/Back-Out Checklist

The Release Management team will deploy the patch PRCA*4.5*317, which is tracked in the NPM in Forum, nationally to all VAMCs. Forum automatically tracks the patches as they are installed in the different VAMC production systems. One can run a report in Forum to identify when the patch was installed in the VistA production at each site, and by whom. A report can also be run, to identify which sites have not installed the patch in their VistA production system as of that moment in time.

Therefore, this information does not need to be manually tracked in the chart below.

Table 6: 3.3.4.1 Deployment/Installation/Back-Out Checklist

Activity	Day	Time	Individual who completed task
Deploy	N/A	N/A	N/A
Install	N/A	N/A	N/A
Back-Out	N/A	N/A	N/A

4 Installation

4.1 Pre-installation and System Requirements

PRCA*4.5*317, a patch to the existing VistA Accounts Receivable 4.5 package, is installable on a fully patched M(UMPS) VistA system and operates on the top of the VistA environment provided by the VistA

infrastructure packages. The later provides utilities which communicate with the underlying operating system and hardware, thereby providing Accounts Receivable independence from variations in hardware and operating system.

4.2 Platform Installation and Preparation

Refer to PRCA*4.5*317 documentation on the National Patch Module (NPM) on Forum for the detailed installation instructions. These instructions would include any pre installation steps if applicable.

4.3 Download and Extract Files

Refer to PRCA*4.5*317 documentation on the NPM for where to find related documentation that can be downloaded. PRCA*4.5*317 will be transmitted via a PackMan message and can be pulled from the NPM. It is not a host file, and therefore does not need to be downloaded separately.

4.4 Database Creation

PRCA*4.5*317 does not modify the VistA database. If it did any changes could be found on the NPM documentation for this patch.

4.5 Installation Scripts

No installation scripts are needed for PRCA*4.5*317 installation.

4.6 Cron Scripts

No Cron scripts are needed for PRCA*4.5*317 installation.

4.7 Access Requirements and Skills Needed for the Installation

The following staff will need access to the PackMan message containing the PRCA*4.5*317 patch or Forum's NPM for downloading the nationally released PRCA*4.5*317 patch. The software is to be installed by the site's or region's designated: VA OI&T IT OPERATIONS SERVICE, Enterprise Service Lines, Vista Applications Division [2].

4.8 Installation Procedure

Refer to PRCA*4.5*317 documentation on the NPM for the detailed installation instructions.

4.9 Installation Verification Procedure

Refer to PRCA*4.5*317 documentation on the NPM for the detailed installation instructions. These instructions would include any post installation steps if applicable.

4.10 System Configuration

No system configuration changes are required for this patch.

---

[2] "Enterprise service lines, VAD" for short. Formerly known as the IRM (Information Resources Management) or IT support.

4.11   Database Tuning

No reconfiguration of the VistA database, memory allocations or other resources is necessary.

5 Back-Out Procedure

Back-Out pertains to a return to the last known good operational state of the software and appropriate platform settings.

5.1 Back-Out Strategy

Although it is unlikely a back-out decision due to major issues with this patch could occur during site Mirror Testing, Site Production Testing or after National Release to the field (VAMCs). The strategy would depend on during which of these stages the decision is made.

If during Mirror testing or Site Production Testing, unless the patch produces catastrophic problems, the normal VistA response would be for a new version of the test patch correcting defects to be produced, retested and upon successfully passing development team testing would be resubmitted to the site for testing. This project, however, has prepared a set of back-out patch instructions if necessary, as in the case that the project is canceled or the implemented design is found to be so wrong and detrimental to the site's delivery of services to veterans that the software must be removed.

If the defect(s) were not discovered until after national release but during the designated support period, a new patch will be entered into the National Patch Module on Forum and go through all the necessary milestone reviews etc. as a patch for a patch. It is up to VA OI&T and product support whether this new patch would be defined as an emergency patch or not. After the support period, the VistA Maintenance Program would produce the new patch, either to correct the defective components or to back-out the patch.

In the case of PRCA*4.5*317, a new patch would not be necessary for back out purposes as the site will have a backup that they created during the initial install.

5.2 Back-Out Considerations

It is necessary to determine if a wholesale back-out/rollback of the patch PRCA*4.5*317 is necessary or if a better course is to correct through a new version of the patch (if prior to national release) or a subsequent patch aimed at specific areas modified or affected by the original patch (after national release). If the back-out is post-release of patch PRCA*4.5*317, this patch should be assigned status of "Entered in Error" in Forum's NPM.

5.2.1   Load Testing

N/A. The back-out process would be executed at normal, rather than raised job priority, and is expected to have no significant effect on total system performance. Subsequent to the reversion, the performance demands on the system would be unchanged.

5.2.2   User Acceptance Testing

For the following three areas in VistA, a user with a preferred view on file should select the menu option or action listed below and confirm that they are no longer prompted with the question "Use preferred view?" prior to the screen displaying the selected data.
   • ERA Worklist [RCDPE EDI LOCKBOX WORKLIST]

- ERA Scratchpad
  - ERA Worklist [RCDPE EDI LOCKBOX WORKLIST] → action 'Select ERA'
- Auto-Post Awaiting Resolution [RCDPE APAR]

User with access to the "EDI Lockbox (ePayments) Reports Menu…" [RCDPE EDI LOCKBOX REPORTS MENU] should pull up the menu and confirm that the "Unapplied EFT Deposits Report" [RCDPE UNAPPLIED EFT DEP REPORT]" option is no longer available.

It is expected that the IT Support can confirm that the option "Unapplied EFT Deposits Report" [RCDPE UNAPPLIED EFT DEP REPORT] has been removed from the VistA system.

5.3 Back-Out Criteria

The project is canceled or the requested changes implemented by PRCA*4.5*317 are no longer desired by VA OI&T and the ePayments eBusiness team.

5.4 Back-Out Risks

Before national release: There are no current identified risks of backing out PRCA*4.5*317 prior to national release.

After national release: If the PRCA*4.5*317 patch is to be backed out after it is nationally released it may do so according to this document **only** if none of the following statements are true. If any of the following statements are true, refer to the sub bullets below for proper guidelines.

- Subsequent patch(es) that is currently under development is dependent upon any aspect changed by PRCA*4.5*317.
  - Inform the teams responsible for the subsequent patch(es) of the request to backout the patch so they can make any necessary changes to their software and schedule. With coordination of these teams for the subsequent patch(es), proceed with the backout.

- Subsequent patch(es) that is nationally released or has the status of 'completed/not released' is dependent upon any aspect changed by PRCA*4.5*317.
  - Back-out procedures may not be executed. This requires a new patch to address the concern.

5.5 Authority for Back-Out

The order would come from: release coordinator (product support), portfolio director and health product support.

5.6 Back-Out Procedure

A few things need to be done in order to back out this PRCA*4.5*317 patch. They are as follows: restore the routines to their previous state, remove an option from a menu, delete an option, and rebuild the menu trees. This will need to be done by the site's designated IT support.

Restore the routines to their previous state
The user was instructed to execute the menu option "Backup a Transport Global" [XPD BACKUP] when the patch was initially installed (the very 1ˢᵗ time if installed multiple times). To restore the routines, locate the MailMan message that was created as part of that step. While viewing the MailMan message,

extract the KIDS build, using the "Xtract PackMan" action. Then select the "INSTALL/CHECK MESSAGE" action to restore the modified routines.

Remove an option from a menu
Within FileMan, use the "ENTER OR EDIT FILE ENTRIES" option and select the file "OPTION" (#.19). When prompted for 'EDIT WHICH FIELD', answer with the "MENU" multiple (#10). When prompted for 'EDIT WHICH MENU SUB-FIELD', answer with "ITEM" (#.01). When prompted for "Select OPTION NAME", answer with "EDI Lockbox (ePayments) Reports Menu…" [RCDPE EDI LOCKBOX REPORTS MENU] and remove/delete the ITEM [RCDPE UNAPPLIED EFT DEP REPORT] "Unapplied EFT Deposits Report".

> ** *IMPORTANT:* If the site added the option "Unapplied EFT Deposits Report" [RCDPE UNAPPLIED EFT DEP REPORT] to any other menus, remove it from those menus as well at this time.

Delete an option
Within FileMan, use the "ENTER OR EDIT FILE ENTRIES" option and select the file "OPTION" (#.19). When prompted for 'EDIT WHICH FIELD', answer with the "NAME" (#.01). When prompted for "Select OPTION NAME", answer with "Unapplied EFT Deposits Report" [RCDPE UNAPPLIED EFT DEP REPORT] . Delete this option. When prompted for "DO YOU WANT THOSE POINTERS UPDATED (WHICH COULD TAKE QUITE A WHILE)?", answer NO.

5.7 Back-out Verification Procedure

It is expected that the IT support can use FileMan to confirm that the menu option "Unapplied EFT Deposits Report" [RCDPE UNAPPLIED EFT DEP REPORT] has been successfully removed from the VistA system.

6 Rollback Procedure

Rollback pertains to data. Since patch PRCA*4.5*317 does not impact the data in the Accounts Receivable package there is no need for a rollback procedure. The back-out procedure includes instructions of how to remove and delete a menu option so no additional procedures are necessary to roll back the VistA software.

6.1 Rollback Considerations

Not applicable.

6.2 Rollback Criteria

Not applicable.

6.3 Rollback Risks

Not applicable.

6.4 Authority for Rollback

Not applicable.

6.5 Rollback Procedure

Not applicable.

6.6 Rollback Verification Procedure

Not applicable.

Template Revision History

Date	Version	Description	Author
March 2016	2.2	Changed the title from Installation, Back-Out, and Rollback Guide to Deployment and Installation Guide, with the understanding that Back-Out and Rollback belong with Installation.	VIP Team
February 2016	2.1	Changed title from Installation, Back-Out, and Rollback Plan to Installation, Back-Out, and Rollback Guide as recommended by OI&T Documentation Standards Committee	OI&T Documentation Standards Committee
December 2015	2.0	The OI&T Documentation Standards Committee merged the existing *"Installation, Back-Out, Rollback Plan"* template with the content requirements in the OI&T End-user Documentation Standards for a more comprehensive Installation Plan.	OI&T Documentation Standards Committee
February 2015	1.0	Initial Draft	Lifecycle and Release Management